


NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

COMMERCIAL SOLUTIONS for CLASSIFIED (CSfC)

Key Management Requirements Annex 3.0.0 DRAFT.1

Version 3.0.0 DRAFT.1
27 February 2025


CHANGE HISTORY

Title	Version	Date	Change Summary
CSfC Key Management Requirement Annex	3.0.0 DRAFT.1	27 February 2025	•Added CNSA Suite 2.0 table of algorithms and added objective requirement • Added clarifying language to requirements based on stakeholder feedback •Added requirement ensuring red and gray management components are issued certificates by different CAs •Replaced “Wireless PSK” with “Wireless Password” •Added verbiage to role-based requirements to clarify separation of Security Administrator role from other roles • Clarified applicability of requirements based on type of CA • Added KM Annex testing requirement • Updated Appendix C: References. • Minor administrative changes were made in formatting and punctuation.
CSfC Key Management Requirements Annex	2.1	19 May 2022	• Relocated KM product selection requirements from all Data-In-Transit CSFC Capability Packages (CPs). • Relocated and updated KM role-based personnel requirements from all CSfC CPs. • Added additional requirements to improve separation of inner and outer Public Key Infrastructures (PKIs). • Added Password/Passphrase Strength Parameters appendix from DAR CP. • Relocated and updated Enterprise Gray KM requirements from CSfC Enterprise Gray Implementation Requirements Annex. • Added additional Certification Authorities deployment options figures. • Updated Appendix C: References. • Minor administrative changes were made in formatting and punctuation.

Title	Version	Date	Change Summary
CSfC Key Management Requirements Annex	2.0	29 January 2021	• Updated based on stakeholder feedback to KM Annex v1.0. • Relocated MACsec pre-shared symmetric Connectivity Association Keys (CAKs) management requirements to CSfC Symmetric Key Management Requirements Annex. • Updated wording in Section 1 to improve clarity. • Removed the use of whitelists as an alternative to Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) Responders for certificate revocation checking. • Updated requirements to align with CNSS Policy (CNSSP) 25 and CNSS Directive (CNSSD) 506. • Updated Appendix B: References. • Minor administrative changes were made in formatting and punctuation.
Commercial Solutions for Classified (CSfC) Key Management Requirements Annex	1.0	26 June 2018	• Initial release of the CSfC Key Management Requirements Annex.

TABLE OF CONTENTS

Table of Figures

List of Tables

1 INTRODUCTION

The Commercial Solutions for Classified (CSfC) Program within the National Security Agency's (NSA's) Cybersecurity Directorate (CSD) publishes guidance to empower its customers to implement secure communication solutions using independent, layered Commercial-off-the-Shelf (COTS) products. This guidance is product-neutral and describes system-level solution frameworks documenting security and configuration requirements for customers and/or integrators.

CSD delivers guidance to meet the needs of customers implementing Key Management (KM) in CSfC data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components.

2 PURPOSE AND USE

KM is implemented as part of a holistic, risk management and defense-in-depth information security strategy integrated into CSfC architectures. Organizations designing CSfC solutions and implementing KM capabilities should leverage information gathered from KM capabilities to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of CSfC systems.

Guidance provided in the KM Annex references architecture and corresponding high-level configuration information to help customers develop a KM solution to meet CSfC KM requirements. To implement a KM solution based on this guidance, all Threshold requirements, or the corresponding Objective requirements, must be implemented as described in Section 6.

The requirements in this document supersede existing KM requirements in published CSfC Capability Packages (CPs). Future CP revisions will direct customers to this annex for KM implementation.

Please provide comments on the usability, applicability, and/or shortcoming of this guidance to an NSA Client Advocate and the KM guidance maintenance team at CSfC_Key_Man_Req_Team@nsa.gov. Solutions adhering to this guidance must also comply with Committee on National Security Systems (CNSS) policies and instruction.

For any additional information on Cross Domain Solutions (CDS) contact the National Cross Domain Strategy Management Office (NCDSMO) at ncdsmo@nsa.gov.

3 LEGAL DISCLAIMER

This guidance is provided "as is". Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a purpose are denied. In no event must the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this guidance, even if advised of the possibility of such damage.

The user of this guidance agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney's fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

This guidance is not intended to constitute an endorsement, explicitly or implied, by the U.S. Government of any manufacturer's product or service.

4 KEY MANAGEMENT OVERVIEW AND REQUIREMENTS

Commercial Solutions for Classified (CSfC) Data-In-Transit (DIT) solutions use asymmetric algorithms, as defined in the Commercial National Security Algorithm (CNSA) Suite, and X.509 certificates for component authentication to establish the Outer and Inner encryption tunnels. Customers protecting long-life[1] classified information should see the *CSfC Symmetric Key Management Requirements Annex* for additional details on how symmetric key cryptography can be leveraged in the Capability Packages (CPs).

Each CSfC DIT encryption component contains a private authentication key and a corresponding public certificate issued by a trusted Certification Authority (CA). It is preferable for the authentication keys (public/private key pair) to be generated on the solution component, where the private keys are never exported out of the component. If the component cannot generate its own key pair, a dedicated offline management workstation is required to generate the key pair for the component. The public keys are sent in certificate requests to a trusted CA that creates and signs authentication certificates containing the public keys. The authentication certificates are then delivered to, and installed on the solution components during provisioning, along with the private keys if they were not generated on the component.

To provide confidentiality services within CSfC DIT solutions, the components use key agreement protocols (such as Elliptic Curve Diffie-Hellman (ECDH)) to generate ephemeral encryption keys. The use of ephemeral encryption keys is not part of key management discussed in this annex.

In CSfC DIT solutions, typically at least two CAs are used to issue certificates and are deployed on separate machines. One CA (known as the Outer CA) issues certificates to Outer Encryption Components and the other CA (known as the Inner CA) is used to issue certificates to Inner Encryption Components. To ensure that the same certificate cannot be used for authenticating both the Outer and Inner tunnels, the Outer CA and Inner CA have different trust chains, respectively. When multiple classified enclaves are used, each enclave will have its own Inner CA, as Inner CAs cannot be shared between multiple classification levels. Additionally, each CSfC solution infrastructure component will have access to revocation status of certificates (e.g., Certificate Revocation List (CRL) or Online Certificate Status Protocol (OSCP)). All certificates issued by the Outer and Inner CAs for the Solution are Non-Person

[1] Long-life is defined as needing protection for 15 years or longer.

Entity (NPE) certificates, except in the case when a Mobile Access (MA) Transport Layer Security (TLS) EUD requires a user certificate for the Inner TLS tunnel.

The CAs that issue authentication certificates to CSfC solution components operate either as Enterprise CAs (i.e., National Security Systems (NSS) Public Key Infrastructure (PKI), National Security Agency (NSA) Key Management Infrastructure (KMI), Intelligence Community (IC) PKI, Department/Agency-level Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs, or locally-run CAs). Existing Enterprise CAs should be used whenever possible, as the advantages for using these CAs outweigh those associated with locally-run CAs. However, Enterprise CAs that operate on or are accessible via the Black Network are not permitted to be used in CSfC solutions. CNSSP 25 is the governing policy and CNSSD 506 is the governing directive for PKI solutions in support of CSfC solutions protecting networks operating at the Secret level (typically the red network of the solution).

Enterprise CAs have established operations, as well as Certificate Policies and Certification Practice Statements (CPSs) that customer organizations can leverage for their CSfC solution. These Enterprise CAs operate at Federal Department and Agency levels (e.g., NSS PKI, KMI, IC PKI), and offer wide-scale interoperability across Department and Agency networks and CSfC solutions (i.e., the certificate policies and their registered policy Object Identifiers (OIDs) are widely accepted across Federal Departments or Agencies). These types of Enterprise solutions, leverage Department/Agency-level trusted CAs that reside under the same Root CA. Enterprise CAs can be used in multiple CSfC solutions throughout Federal Departments or Agencies, thereby providing certificate trust interoperability across those CSfC solutions. A user with a CSfC device provisioned with certificates from an Enterprise CA could use their device in many different CSfC solutions deployed throughout Federal Departments or Agencies. CSfC solutions utilizing Enterprise CAs install the Issuing CA and Root CA certificates into solution components so that a trusted certificate chain is established between the component certificate and the trusted Root CA certificate.

Departments and Agencies can also deploy Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs to support the need to issue certificates to NPEs that will only be trusted within the Department/Agency network. NPE OLT CAs can be operated as standalone systems or can be part of a Department/Agency NPE OLT PKI. All CAs within an NPE OLT PKI must meet the guidelines as stated in CNSSD 506.

CSfC solutions can also deploy and operate their own locally-run CAs for closed operational networks that are independent of any Enterprise CAs. In this configuration, certificate policy and interoperability are constrained to the specific CSfC solution. Furthermore, the CSfC solution owner is required to develop and maintain CPSs that detail the operational procedures for the locally-run CAs. In addition, the customer may need to develop and maintain a higher-level Certificate Policy if one does not already exist.[2] Table 1 summarizes the differences between Enterprise and locally-run CAs.

[2] *CNSSP 25 is the governing policy for PKI solutions in support of Secret CSfC solutions. For CSfC solutions that are higher than Secret, the CSfC solution owner is required to develop a Certificate Policy that is approved by the local Approving Official (AO).*

Table 1. Certification Authority Deployment Options

CA Type	Certificate Policy/ Certification Practice Statement	Interoperability	Operations
Enterprise CAs	Owned and managed by the Enterprise PKI (e.g., NSS PKI, NSA KMI, IC PKI)	Across Department and Agency networks	Performed by the Enterprise PKI and Departments/Agencies
Department/ Agency-level Non-Person Entity (NPE) Only Locally Trusted (OLT) CAs	Owned and managed at the Department or Agency level	Constrained to a Department or Agency network	Performed by the Department or Agency
Locally-run (Non-Enterprise) CAs	Owned and managed at the CSfC solution level	Constrained to a CSfC solution	Performed by the CSfC solution owner

In all CA configurations identified above, Outer CAs issue and manage authentication certificates for Outer Encryption Components and Gray Management Service Components; Inner CAs issue and manage authentication certificates for Inner Encryption Components and Red Management Service Components. Outer CAs can be included as either part of the Gray Network or Red Network. If the solution supports multiple classified enclaves, the Outer CA is located either in the Gray Management Network or in the Red Network of the highest classified enclave. Inner CAs can only be located in the Red Network.

If CAs are part of a CSfC Multi-Site Connectivity (MSC) Solution, each site has the option of using either locally-run CAs that they manage and control or, where available, enterprise CAs that are not necessarily managed by the Solution Owner. Any Encryption Components at each site using public key certificates need to have the signing certificates and revocation information for the corresponding CAs used by the other sites in the MSC Solution. This high-level design requires cooperation between the various sites in the solution to ensure that all CAs used by each site are trusted at all the other sites. If remote central management is used in an MSC solution, personnel at a single geographic site administer and perform certificate issuing and management for all the sites included in the solution.

For CSfC solutions that deploy central Gray Network management in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) uses a certificate issued by a different CA than the Inner CA for authentication. The Gray Firewall and the Outer Encryption Component can both use certificates issued by the same Outer CA for authentication.

The CAs communicate with management services (e.g., Device Managers (DMs), Registration Authorities (RAs)) deployed in the corresponding network to support enrollment and life-cycle certificate management for CSfC solution components. Outer and Inner CAs in the Red Network are limited to directly communicating with Red Management Services. Outer CAs in the Gray Network are limited to directly communicating with Gray Management Services. When the CA is not located in the same network as the Management Services, an Authorizing Official (AO)-approved method (e.g., CDS) can be used allowing indirect communication (for example Certificate Enrollment). The Red and Gray

Management Services enable the certificate request/response process between a CSfC solution component and a CA.

An out-of-band method is used to issue the initial certificates to the solution components. Subsequent rekeying, however, can take place over the network through the solution prior to the current key's expiration (see Section 2 for additional details regarding over-the-network remote certificate rekey). The key validity period for certificates issued by locally run CAs does not exceed 14 months for EUDs and 24 months for Solution Infrastructure Components, while the key validity period for certificates issued by an Enterprise CA are inherited from the Enterprise CA certificate policy. Updates to CRLs are distributed to Outer and Inner Infrastructure Encryption components within 24 hours of CRL issuance.

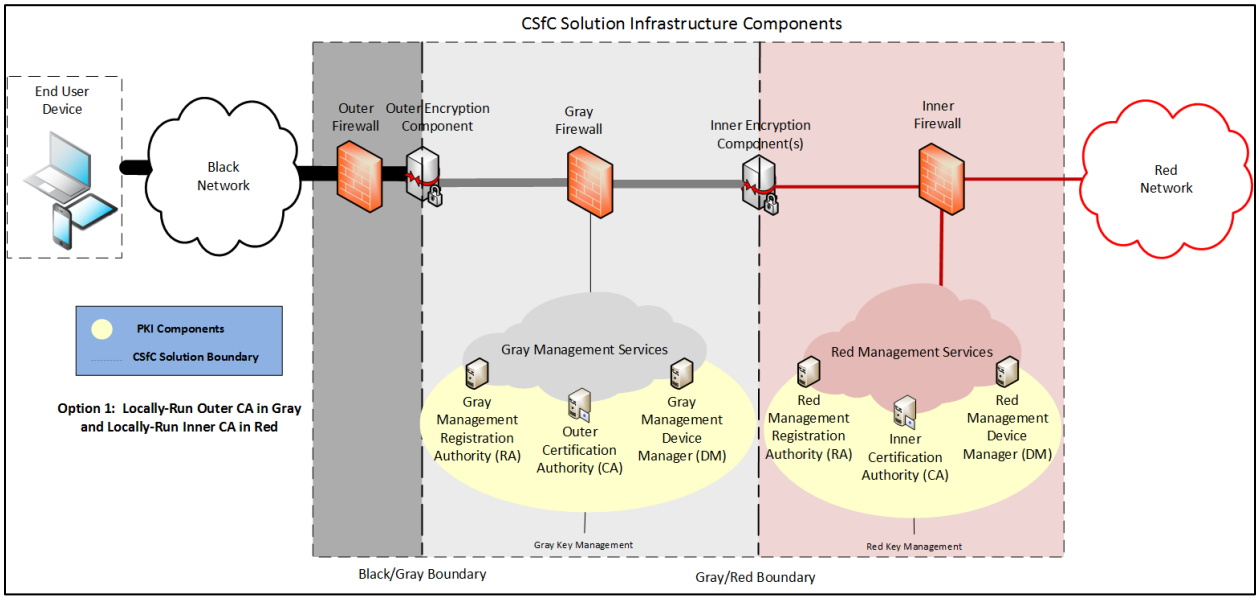
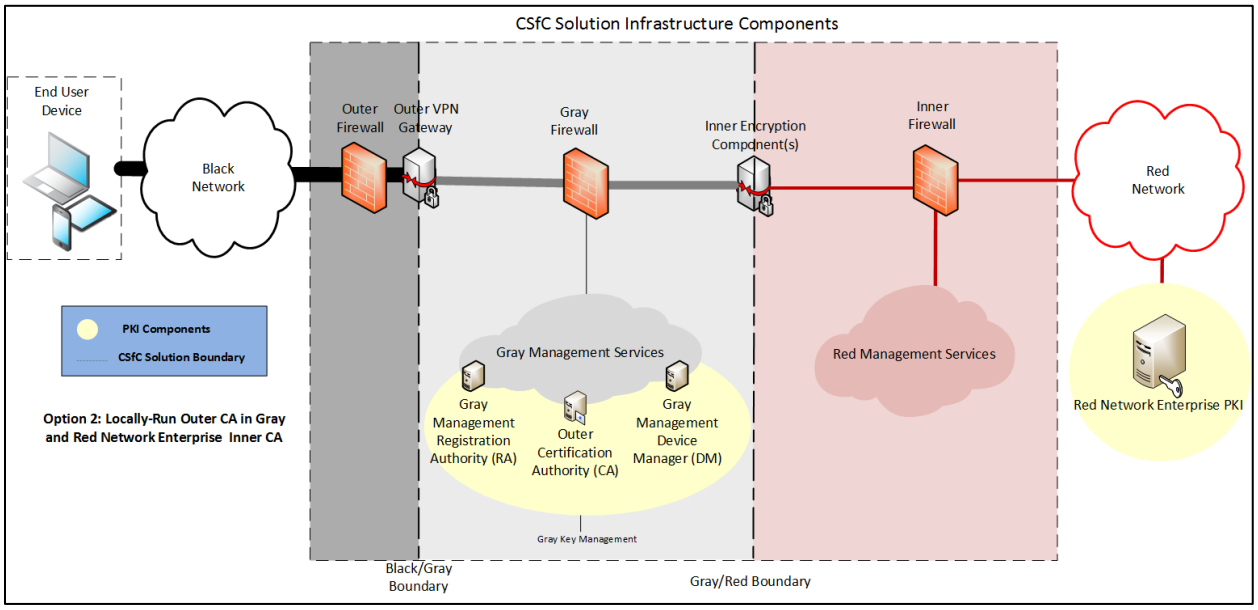


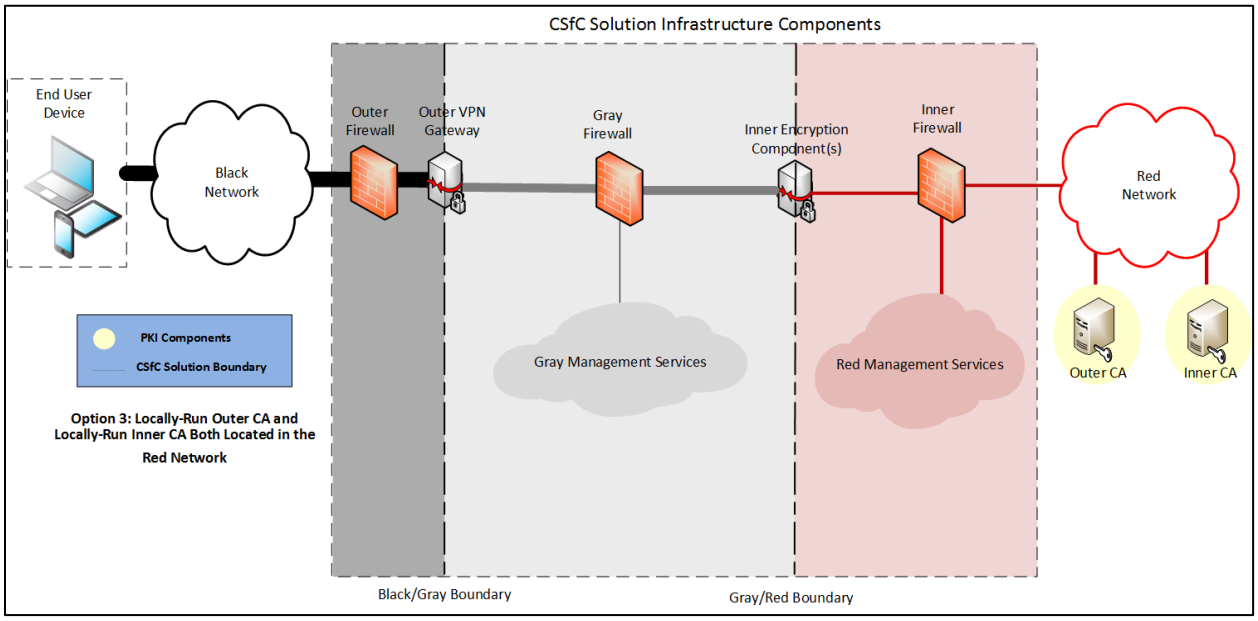
Figure 1. Locally-Run Outer CA in Gray and Locally-Run Inner CA in Red



160

161 **Figure 2. Locally-Run Outer CA in Gray and Red Network Enterprise Inner CA**

162

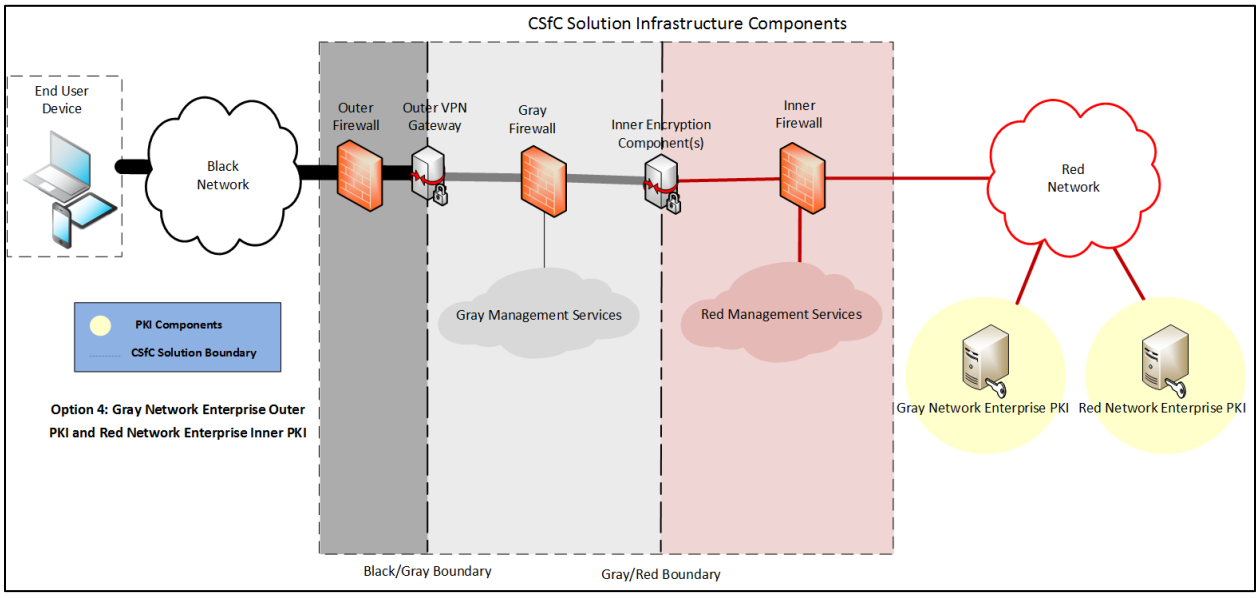


163

164 **Figure 3. Locally-Run Outer CA and Locally-Run Inner CA Both Located in the Red**
165 **Network on Physically Separate Machines**

166

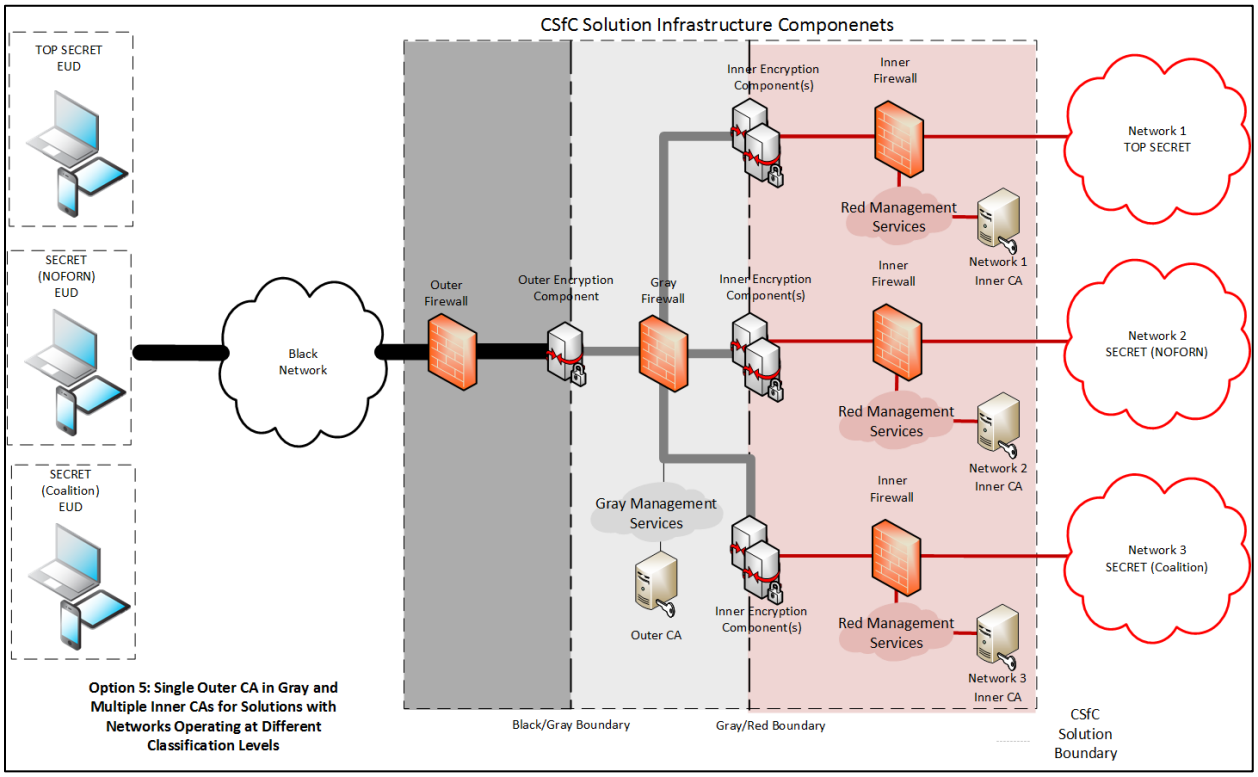
167



168

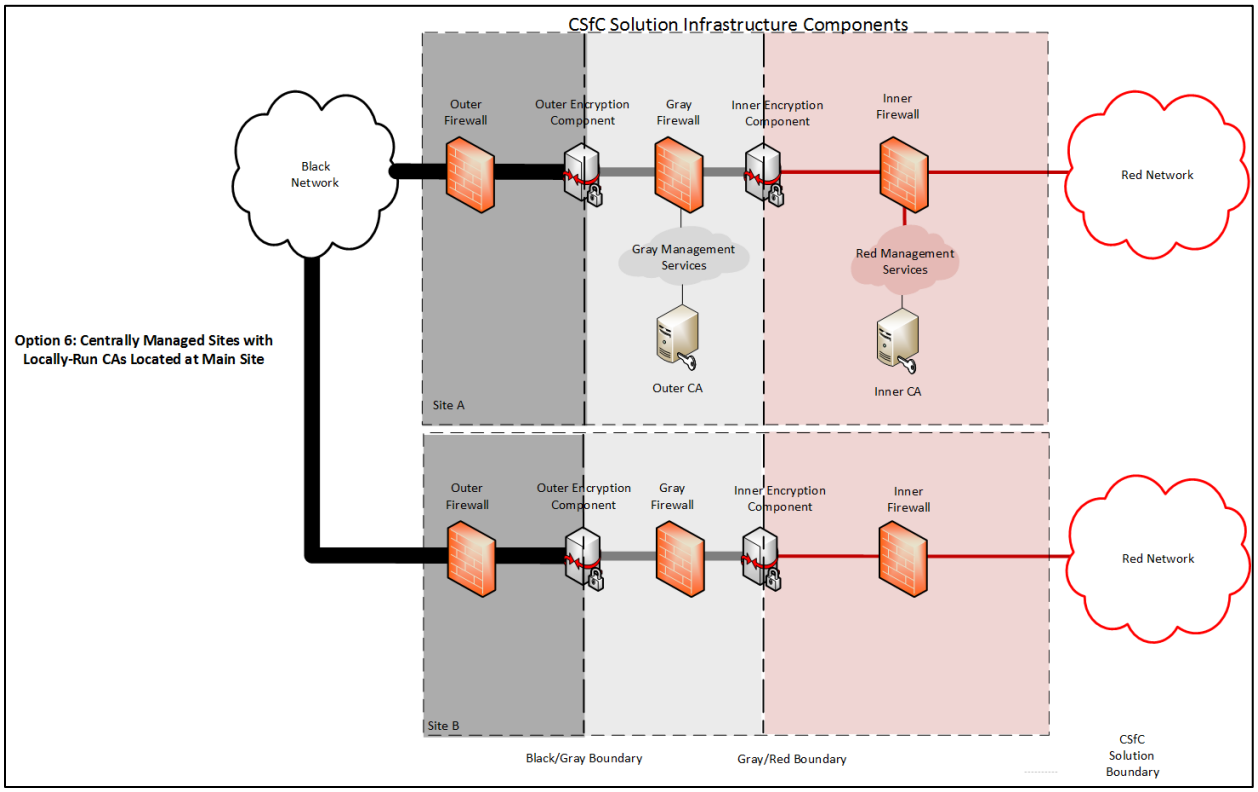
169 **Figure 4. Gray Network Enterprise Outer PKI and Red Network Enterprise Inner PKI**

170



171

172 **Figure 5. Single Outer CA in Gray and Multiple Inner CAs for Solutions with Networks**
173 **Operation at Different Classification Levels**



174

175 **Figure 6. Centrally Managed Sites with Locally-Run CAs Located at Main Site**

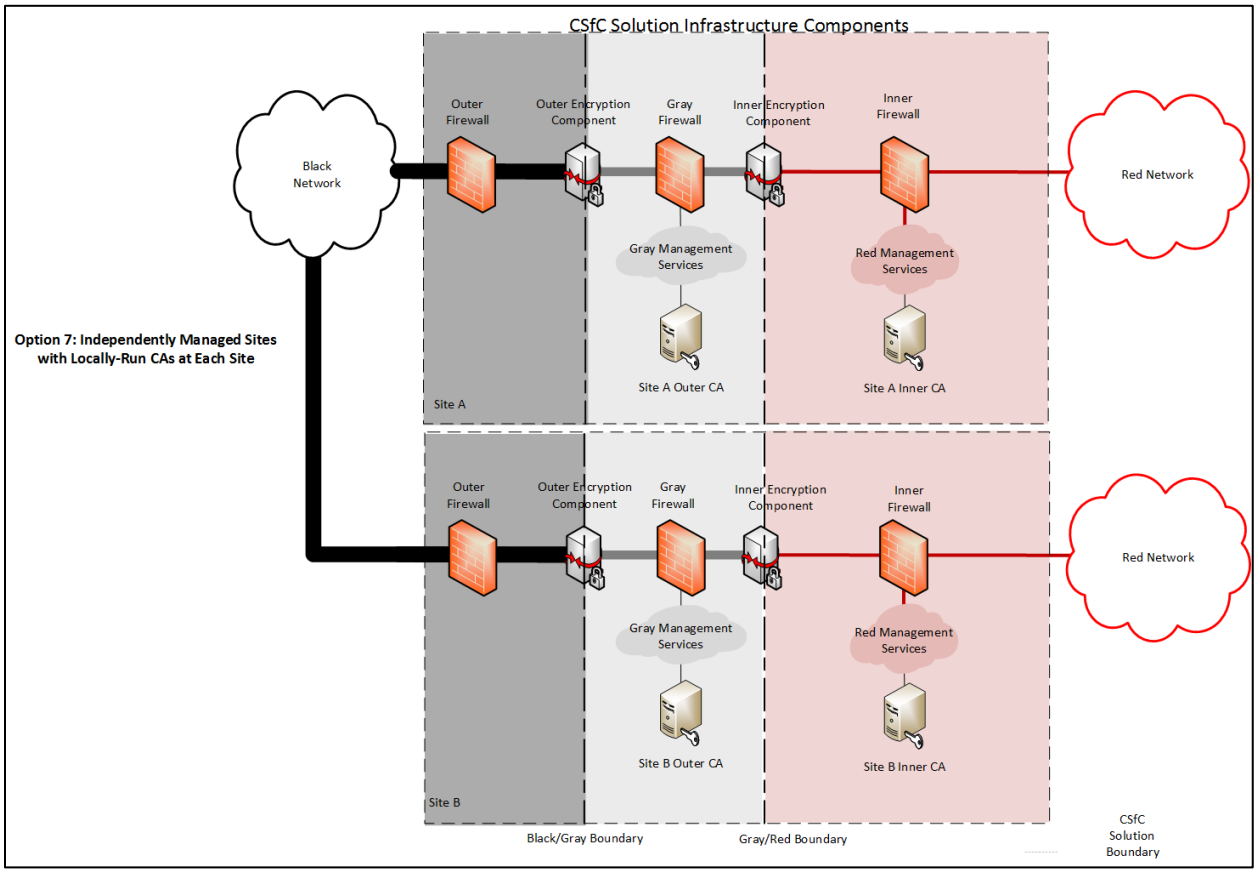


Figure 7. Independently Managed Sites with Locally-Run CAs at Each Site

4.1 Certificate Revocation Checking

CRLs are used by CAs to convey the revocation status of certificates issued by those CAs, and those CRLs need to be made available to the CSfC solution components.

A CRL Distribution Point (CDP) is a web server whose sole function is to provide external distribution of, and access to CRLs issued by CAs. CDPs do not serve any other purpose, and in particular, do not host any dynamically generated content. CDPs also do not provide any other services other than the distribution of CRLs. CDPs are optional in a CSfC solution, and they can exist in the Gray and/or Red Networks. An AO approved method is needed to periodically distribute the current CRL from the CA to the CDP server on the same or different networks. Alternatives to CDPs include Online Certificate Status Protocol (OCSP) Responders and locally-stored or cached CRLs.

The Outer Encryption Component in the solution infrastructure accesses an Outer CDP, located in the Gray Network, to obtain CRLs and check revocation status of other Outer Encryption Components, and EUDs when applicable, prior to establishing the Outer encryption tunnel. Furthermore, a CDP operating in the Gray Network can be accessed by Gray Management Services Components to obtain CRLs and check the revocation status of the Outer Encryption Component's certificate prior to establishing a device management tunnel with the Outer Encryption Component.

Additionally, the CSfC CPs allow for an Inner CDP to be located within the Gray Network. Placing an Inner CDP in the Gray Network allows devices to check the certificate status of the Inner Encryption Component prior to establishing a tunnel. To use an Inner CDP in the Gray Network, an AO determines that CRLs generated by the Inner CA are unclassified. These CRLs are moved from the Red Network to the Gray Network using an AO approved method (e.g., CDS).

Inner Encryption Components access an Inner CDP, located in the Red Network, to obtain CRLs and check revocation status of other Inner Encryption Components, and EUDs when applicable, prior to establishing the Inner encryption tunnel. Likewise, a CDP operating in the Red Network can be accessed by Red Management Services Components to obtain CRLs and check the revocation status of the Inner Encryption Component's certificate prior to establishing a device management tunnel with the Inner Encryption Component.

An Outer CDP and an Outer CA can reside on the same or different networks. For example, the Outer CA can operate in the Red Network, while the Outer CDP operates in the Gray Network. If they reside on different networks, an AO approved method (e.g., CDS) is needed to periodically distribute the current CRL from the CA to the CDP.

CRLs are downloaded by CSfC solution components over unencrypted Hypertext Transfer Protocol (HTTP). A CRL's integrity is protected by the digital signature of the issuing CA, and additional integrity protection during CRL download is not required. Placement of CDPs on the Gray Network for the Outer Encryption Component and Red Network for Inner Encryption Components reduces the exposure to external threat actors.

To provide redundancy and ensure that current CRLs are always made available to CSfC solution components, multiple Outer and Inner CDPs can be deployed. The use of multiple CDPs is left to the discretion of the CSfC solution owner. Furthermore, CDPs can host partition or delta CRLs in addition to complete CRLs. In large CSfC solutions, the use of partition or delta CRLs can reduce the amount of network traffic needed to distribute updates to CRLs. A CA's Certificate Policy will define whether the use of partition or delta CRLs is permissible.

OCSP Responders or locally-stored/cached CRLs can be used in lieu of CDP Servers. OCSP Responders located in the Gray Network can provide certificate revocation status information to the Outer Encryption Components or to the Authentication Server. Additionally, OCSP Responders in the Red Network can provide certificate revocation status information to Inner Encryption Components.

4.2 Wireless Key and Certificate Management

4.2.1 Mobile Access (MA) CP

As discussed in the Black Network section of the MA CP, EUDs can operate over any Black Network when used in conjunction with a Government-owned Retransmission Device (RD) or a physically separate Dedicated Outer VPN to establish the Outer IPsec Tunnel. When the RD or Dedicated Outer VPN is

wirelessly connected to an EUD using Wi-Fi, the Wi-Fi connection should implement Wi-Fi Protected Access III (WPA3) with a wireless password.

For WPA3 or WPA2 with passwords, a common password with at least 256 bits of security needs to be securely generated, distributed, and installed onto both the EUD and the external Dedicated Outer VPN device or RD. Exposure of the password in red form needs to be minimized to the greatest extent possible and only exposed to authorized and trusted personnel responsible for managing and installing the PSK onto the EUD and external Dedicated Outer VPN or RD. Updates to the password are to be performed periodically based upon the threat environment. The higher the threat environment, the more often the password should be updated.

4.2.2 Campus Wireless Local Area Network (WLAN) CP

Since the *Campus Wireless Local Area Network (WLAN) CP* relies on WPA3 Enterprise for the Outer Encryption tunnel, the EUD will require an EAP-TLS certificate. This certificate is issued by the Outer CA. Issuance of the WPA3 Enterprise certificate should be integrated into the overall provisioning process for the EUD described in the EUD Provisioning section of the CPs. For the WLAN CP, revocation status information for EAP-TLS certificates issued to EUDs also needs to be made available in the Gray Network so that the WPA3 Enterprise authentication server can check the revocation status of EUD EAP-TLS certificates (see Section 1.1 for additional details regarding distribution of CRLs).

5 REMOTE REKEY OF COMPONENT CERTIFICATES

If a solution component is capable of generating its own public/private key pairs and can communicate with the Outer or Inner CAs using Enrollment over Secure Transport (EST), as defined in Internet Engineering Task Force (IETF) RFC 7030, the solution component can have its device certificates remotely rekeyed, as opposed to physically returning the solution component to the provisioning environment as described in the provisioning section of the CPs. EST requires a TLS connection to a trusted server, so that the CA can authenticate a solution component prior to issuing new certificates. A solution component would need to establish a separate TLS tunnel to the Outer CA or Inner CA after establishing the Outer and Inner encryption tunnels.

Once authenticated to the Outer CA or Inner CA, the solution component generates a new public/private key pair. The newly generated public key is placed into a new certificate request in accordance with RFC 7030. The certificate request is then submitted to the Outer CA or Inner CA for processing using EST. The CA validates that the certificate requests came from a valid and authenticated solution component, processes the certificate request, and returns a newly signed certificate containing the new public key to the solution component. The solution component then receives and installs the newly rekeyed certificate. All CSfC EST implementations use CNSA TLS 1.2 (at a minimum) certificate-based authentication as stated in RFC 9151.

It should be noted that the exact sequence for certificate rekey will vary based on the solution component's implementation of EST. For example, one certificate rekey with one of the CAs may need to be performed first, followed by the second certificate rekey with the other CA.

6 KEY MANAGEMENT GENERAL REQUIREMENTS

The following requirements apply to all CSfC CPs unless the requirement number identifies a specific CP that the requirement applies to (e.g., WLAN-KM-1 only applies to the WLAN CP).

Multiple versions of a requirement may exist in this Annex, with alternative versions designated as being either a Threshold requirement or an Objective requirement:

- A Threshold (T) requirement specifies a feature or function that provides the minimal acceptable capability for the security of the solution.
- An Objective (O) requirement specifies a feature or function that provides the preferred capability for the security of the solution.

In general, when separate Threshold and Objective versions of a requirement exist, the Objective requirement provides a higher degree of security for the solution than the corresponding Threshold requirement. However, in these cases, meeting the Objective requirement may not be feasible in some environments or may require components to implement features that are not yet widely available. Solution owners are encouraged to implement the Objective version of a requirement, but in cases where this is not feasible, solution owners may implement the Threshold version of the requirement instead. These Threshold and Objective versions are mapped to each other in the "Alternatives" column. Objective requirements that have no related Threshold requirement are marked as "Objective Requirement, No Threshold' in the "Alternatives" column.

In most cases, there is no distinction between the Threshold and Objective versions of a requirement. In these cases, the "Threshold/Objective" column indicates that the Threshold equals the Objective (T=O). Such requirements must be implemented in order to comply with this Annex.

Requirements that are listed as Objective in this Annex may become Threshold requirements in a future version of this Annex. Solution owners are encouraged to implement Objective requirements where possible in order to facilitate compliance with future versions of this Annex.

The "CA Type" column in the requirements tables identifies which CA type, as defined in Section 4 and Table 1, the requirement applies.

6.1 PRODUCT SELECTION REQUIREMENTS

Table 2. Product Selection Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	**CA Type**
KM-PS-1	The products used for the Inner and Outer CAs (e.g. Roots, Intermediates, Issuing CAs) must either be chosen from the list of CAs on the CSfC Components List or the CAs must be NIAP Certified pre-existing Enterprise CAs of the applicable network (i.e. Red Network Enterprise PKI is used for Inner CA and/or Gray Network Enterprise PKI is used for Outer CA).	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-PS-2	The Inner and the Outer CAs must follow one of the following guidelines: • The CAs come from different manufacturers, where neither manufacturer is a subsidiary of the other. • The CAs are different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.	O	Objective Only	All
KM-PS-3	Black Network Enterprise PKI is prohibited from being used as the Outer or Inner tunnel CA.	T=O		All

305

306 ## 6.2 PKI GENERAL REQUIREMENTS

307 **Table 3. PKI General Requirements**

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-1	All public keys and certificates must be treated (e.g., classification level) as determined by the AO.	T=O		All
KM-2	Outer CAs must provide services through either the Gray or Red Network.	T=O		All
KM-3	Inner CAs must provide services through the Red Network.	T=O		All
KM-4	Locally-run Inner CAs must be physically separate from locally-run Outer CAs.	T=O		Locally-run
KM-5	All certificates issued by the Outer and Inner CAs for the Outer and Inner Encryption Tunnels in the Solution must be Non-Person Entity (NPE) certificates, except in the case when a TLS EUD requires a user certificate for the Inner TLS tunnel.	T=O		All
KM-6	All certificates issued by the Outer and Inner CAs for the solution must be used for authentication only.	T=O		All
KM-7	Trusted personnel must be used for administrative access to the CAs.	T	KM-15	All
KM-8	All certificate profiles for the Outer and Inner CAs for the solution must comply with IETF RFC 5280 and IETF RFC 8603.	T=O		All
KM-9	All private keys must be classified as determined by the AO and compliant with CNSSI 4005 (see paragraph 107.e, and section XIII.A.).	T=O		All
KM-10	The key sizes and algorithms for CA certificates (e.g.. Roots, Intermediates, Issuing CAs) and authentication certificates issued to Outer Encryption Components, Inner Encryption Components, and Administrative Device Components must be as specified in Table 4.	T	KM-26	All

Req #	Requirement Description	Threshold / Objective	Alternative	**CA Type**
KM-11	Outer and Inner CAs must not have access to private keys used in the Solution Components.	T=O		All
KM-12	Private keys associated with on-line (i.e., CA is network-accessible), Outer and Inner CAs must be protected using Hardware Security Modules (HSMs) validated to Federal Information Processing Standards (FIPS) 140-2/3 Level 2 or greater.	T=O		All
KM-13	Outer and Inner CAs must have and operate in compliance with a Certificate Policy and Certification Practice Statement that are: • Formatted in accordance with IETF RFC 3647 and NIST IR 7924. • Approved by the AO. • Compliant with CNSSP 25 and the other requirements of this Annex.	T=O		All
KM-14	CAs must run AO-approved anti-virus software.	T=O		All
KM-15	Trusted personnel under two-person integrity (TPI) procedures must be used for administrative access to the CAs.	O	KM-7	All
KM-16	If multiple Red enclaves exist in the Solution and the Outer CA resides in the Red Network, the Outer CA must reside in the Red Network with the highest classification level.	T=O		All
KM-17	Certificate Management Services for the inner tunnel must be provided through the Red Network.	T=O		All
KM-18	Certificate Management Services for the outer tunnel must be provided through either the Gray Network or Red Network.	T=O		All
KM-19	Withdrawn			
KM-20	If the Certificate Management Services operate at the same security level as a Red Network, a Controlled Interface must be used to control information flow between the Certificate Management Services and the Red Network.	T=O		All
KM-21	If the Certificate Management Services operate at a different security level than a Red Network or Gray Network, a CDS Controlled Interface must be used to control information flow between the Certificate Management Services and the Red Network or Gray Network.	T=O		All
KM-22	Copies of CA's own private keys must only be made using AO-approved procedures to support CA continuity of operations and disaster recovery (i.e., backups of private keys or HSMs).	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-23	When multiple classified enclaves are used, each enclave must have its own separate Inner CA, as Inner CAs cannot be shared between multiple classification levels.	T=O		All
KM-24	Inner and Outer CAs must not be signed by the same Root CA.	T=O		All
KM-25	The AO and Information Owner must determine whether long-life[3] classified information exists on the network(s) being accessed and/or is processed/transmitted within the CSfC Solution. If the information is determined to be long-life, then the guidance and requirements in the *CSfC Symmetric Key Management Requirements Annex* should be followed.	T=O		All
KM-26	The key sizes and algorithms for CA certificates (e.g. Roots, Intermediates, Issuing CAs) and authentication certificates issued to Outer Encryption Components, Inner Encryption Components, and Administrative Device Components must be as specified in Table 5.	O	KM-10	All

308

309 **Table 4. Commercial National Security Algorithm (CNSA) Suite 1.0**

Algorithm	Function	Specification	Parameters
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm for key establishment	NIST SP 800-56A	Curve P-384 for all classification levels.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Curve P-384 for all classification levels.
RSA	Asymmetric algorithm used for key-establishment	NIST SP 800-56B	Minimum 3072-bit modulus for all classification levels.
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072-bit modulus for all classification levels.
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels

[3] Long-life is defined as needing protection for 15 years or longer.

Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

310

311 **Table 5. Commercial National Security Algorithm (CNSA) Suite 2.0**

Algorithm	Function	Specification	Parameters
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS 203	Category 5 parameters, ML-KEM-1024 for all classification levels.
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS 204	Category 5 parameters, ML-DSA-87 for all classification levels.
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

312

313 ## 6.3 CERTIFICATE ISSUANCE REQUIREMENTS

314 **Table 66. Certificate Issuance Requirements**

315 (Note: requirements KM-CI-1 to KM-CI-24 previously numbered KM-23 to KM-46)

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-CI-1	EUDs, Outer Components, Inner Components, and Gray and Red Management Services Components must be initially keyed and loaded with certificates using an out-of-band process within a physical environment certified to protect the highest classification level of the solution network.	T=O		All
KM-CI-2	Private keys for EUDs, Outer Components, Inner Components and Gray and Red Management Services Components must never be escrowed.	T=O		All
KM-CI-3	Outer and Inner CAs must use Public Key Cryptographic Standard (PKCS) #10 and PKCS#7 to receive certificate signing requests and issue authentication certificates, respectively, to EUDs, Outer Components, Inner Components, and Gray and Red Management Services Components, or the dedicated offline workstation as detailed in KM-CI-4.	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	**CA Type**
KM-CI-4	If devices cannot generate their own key pairs, a dedicated offline management workstation must be used to generate the key pairs and PKCS#12 must be used for installing certificates and their corresponding private keys to devices.	T=O		All
KM-CI-5	PKCS#12 files for Inner and Outer encryption tunnel authentication certificates must be securely distributed and use random passwords with a minimum length as defined in Appendix A.	T=O		All
KM-CI-6	If devices are capable of generating their own key pairs, Red and Gray Management Services must use PKCS#7 for installing certificates to devices.	T=O		All
KM-CI-7	Withdrawn			
KM-CI-8	Certificate signing requests must be submitted to the CA by an authorized entity and in accordance with the CA's Certificate Policy and CPS. The Solution Owner must identify the authorized entity (e.g. person or software).	T=O		All
KM-CI-9	Outer and Inner CAs must issue certificates in accordance with their Certificate Policies and CPSs.	T=O		All

KM-CI-10	Certificate Policies and CPSs for non-Enterprise, locally-run CAs must ensure the CAs issue certificates within a defined and limited name space and assert:
	• Unique Distinguished Names (DNs)
	• Appropriate key usages
	• A registered certificate policy OID
	• A registered certificate policy OID is not required if all of the following are true:
	  • The certificates are limited to the specific customer's solution. That is, they are not part of an enterprise solution with multiple customers.
	  • The certificates only apply to a single security domain (e.g., Secret).
	  • There is only one certificate type (e.g., device, not user).
	  • There is only one issuance process described in the CP/CPS.
	  • There in only one assurance level.
		T=O		Locally-run

KM-CI-11	If using CDPs, Inner and Outer CAs must assert at least one CRL CDP Uniform Resource Locater (URL) in certificates issued to EUDs, Outer components, Inner Components, and Gray and Red Management Services Components. The CDP URL specifies the location of the CAs' CRL Distribution Point.	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-CI-12	The key validity period for certificates issued by non-Enterprise, locally run CAs to End User Devices must not exceed 14 months.	T=O		Locally-run
KM-CI-13	The key validity period for certificates issued by non-Enterprise, locally run CAs to Solution Infrastructure Components must not exceed 24 months.	T=O		Locally-run
KM-CI-14	Inner CAs must only issue certificates to Inner Components and Red Network Components of the Solution.	T=O		All
KM-CI-15	Outer CAs must only issue certificates to Outer Encryption Components and Gray Network Components of Solutions.	T=O		All
KM-CI-16	Withdrawn			
KM-CI-17	Certificates issued to Outer VPN Gateways must assert the IP address of the Outer VPN gateway in either the Common Name field of the Distinguished Name, or the Subject Alternative Name certificate extension.	O	Objective Only	All
KM-CI-18	The Inner Encryption Component must only establish Inner Encryption Tunnels using certificates issued by the Inner CA.	T=O		All
KM-CI-19	Outer Encryption Components must only establish Outer Encryption Tunnels using certificates issued by the Outer CA.	T=O		All
KM-CI-20	Withdrawn/Replaced by KM-RK-5.			
KM-CI-21	Certificate signing requests submitted to the CA must be approved by an authorized Registration Authority (RA). The CSfC solution owner must identify authorized RAs to approve certificate requests.	T=O		All
KM-CI-22	RAs must use multi-factor authentication to approve certificate requests.	O		All
KM-CI-23	Requirement replaced by EG-KM-1.			
KM-CI-24	Requirement replaced by KM-23.			
KM-CI-25	The CA used for issuing certificates to Red Management Components must be a different CA used for issuing certificates to Grey Management Components.	T=O		All

6.4 CERTIFICATE REKEY REQUIREMENTS

Table 77. Certificate Rekey Requirements

(Note: requirements KM-RK-1 to KM-RK-4 previously numbered KM-47 to KM-50)

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-RK-1	Certificate rekey should occur prior to a certificate expiring. If rekey occurs after a certificate expires, then the initial certificate issuance process must be used to rekey the certificate.	T=O		All
KM-RK-2	Certificate rekey must be performed in accordance with the CA's Certificate Policy and CPS.	T=O		All
KM-RK-3	Inner and Outer CAs must receive certificate signing requests and issue rekeyed authentication certificates to Solution Components using PKCS#10 and PKCS#7, respectively, through an out-of-band process.	T	KM-RK-4 KM-RK-5	All
KM-RK-4	Inner and Outer CAs must support over-the-network rekey of authentication certificates to Solution Components using EST (IETF RFC 7030 using CNSA TLS 1.2 (at a minimum) certificate-based authentication as stated in RFC 9151).	O	KM-RK-3 KM-RK-5	All
KM-RK-5	If over-the-network rekey of certificates to devices occurs over an untrusted network, it must be done using two valid encryption layers to the device in cases where EST in not supported.	O	KM-RK-3 KM-RK-4	All

6.5 CERTIFICATE REVOCATION AND CDP REQUIREMENTS

Table 88. Certificate Revocation and CDP Requirements

(Note: requirements KM-CR-1 to KM-CR-31 previously numbered KM-51 to KM-81)

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-CR-1	Inner and Outer CAs must revoke a certificate issued to Solution Components when the binding between the subject information and public key within the certificate issued is no longer considered valid.	T=O		All
KM-CR-2	Inner and Outer CAs must make certificate revocation information available in the form of CRLs signed by the CAs.	T=O		All
KM-CR-3	CRLs must be X.509 v2 CRLs as defined in ITU-T Recommendation X.509.	T=O		All
KM-CR-4	CRL profiles must comply with IETF RFC 5280 and IETF RFC 8603.	T=O		All
KM-CR-5	Procedures for requesting certificate revocation must comply with the CA's Certificate Policy and Certification Practices Statement.	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	**CA Type**
KM-CR-6	Certificate Policies and CPSs for non-Enterprise, locally run CAs must ensure revocation procedures address the following: • Response for a lost, stolen or compromised device • Removal of a revoked infrastructure device (e.g., VPN Gateway) from the network • Re-establishment of a Solution Component whose certificate was revoked • Revocation of certificates due to compromise of a device • Revocation of an authentication certificate if simultaneous use of the certificate is detected from different IP Addresses	T=O		Locally-run
KM-CR-7	Inner and Outer CAs must make CRLs available to authorized CRL Distribution Points (CDPs) or to Solution Encryption Components to be locally-stored or cached, so that the CRLs can be accessed by Solution Encryption Components.	T	KM-CR-13	All
KM-CR-8	Enterprise CAs must create and publish CRLs in accordance with the Enterprise CAs' Certificate Policies and CPSs.	T=O		Enterprise and Department / Agency-level (NPE) (OLT) CAs
KM-CR-9	Non-enterprise, locally-run CAs must publish new CRLs at least once every 31 days.	T=O		Locally-run
KM-CR-10	Non-enterprise, locally-run CAs must publish a new CRL within one hour of a certificate being revoked.	T=O		Locally-run
KM-CR-11	Solution Infrastructure Components must have access to new certificate revocation information within 24 hours of the CA publishing a new CRL.	T=O		All
KM-CR-12	Non-enterprise, locally run CAs must ensure that new CRLs are published at least 7 days prior to the next update date of the current CRLs.	T=O		Locally-run
KM-CR-13	The Solution must provide certificate revocation status information via an Online Certificate Status Protocol (OCSP) Server on the Red and Gray Networks that is compliant with IETF RFC 6960.	O	KM-CR-7	All
KM-CR-14	Certificate revocation status messages delivered by an OCSP server must be digitally signed and compliant with IETF RFC 6960.	T=O		All
KM-CR-15	Withdrawn			

Req #	Requirement Description	Threshold / Objective	Alternative	**CA Type**
KM-CR-16	If OCSP Responders are used, Inner CAs must assert the Authority Information Access certificate extension and include the list of URLs identifying the Inner OCSP Responders from which Inner VPN Gateways can request and receive OCSP revocation status responses.	T=O		All
KM-CR-17	If OCSP Responders are used, Outer CAs must assert the Authority Information Access certificate extension and include the list of URLs identifying the Outer OCSP Responders from which Outer VPN Gateways can request and receive OCSP revocation status responses.	T=O		All
KM-CR-18	If using CDPs, CRLs hosted by CDPs must be compliant with IETF RFC 5280 and RFC 8603.	T=O		All
KM-CR-19	If using CDPs, CRLs hosted on Inner CDPs must be signed by the associated Inner CA.	T=O		All
KM-CR-20	If using CDPs, CRLs hosted on Outer CDPs must be signed by the associated Outer CA.	T=O		All
KM-CR-21	If using a CDP/OCSP Responder, CDPs and OCSP Responders must only issue CRLs and OCSP responses, respectively, to relying parties over port 80 (HTTP).	T=O		All
KM-CR-22	CRLs must be transferred via an AO approved method from Inner CAs to associated Inner CDP servers and/or Inner OCSP Responders or to Solution Encryption Components if using locally-stored/cached CRLs.	T=O		All
KM-CR-23	CRLs must be transferred via an AO approved method from Outer CAs to associated Outer CDP servers and/or Outer OCSP Responders or to Solution Encryption Components if using locally-stored/cached CRLs.	T=O		All
KM-CR-24	Newly issued CRLs must be transferred to CDP servers and/or OCSP Responders, or to Solution Encryption Components if using locally-stored/cached CRLs, at least 4 days prior to the next update date of the current CRLs.	T=O		All
KM-CR-25	If using a CDP/OCSP Responder, Solution Encryption Components must attempt to download the latest CRL from a CDP or an OCSP response from an OCSP Responder at least once every 24 hours.	T=O		All
KM-CR-26	Withdrawn			
KM-CR-27	If using a CDP/OCSP Responder, CDPs and OCSP Responders must only accept management traffic over TLS 1.2 (or later version) or Secure Shell (SSH)v2.	T=O		All

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-CR-28	If using a CDP/OCSP Responder, CDPs and OCSP Responders must only accept connections from authorized Solution Components or Administration Workstation addresses or address ranges.	T=O		All
KM-CR-29	If using a CDP/OCSP Responder and an integrity check of a CRL or OCSP response received from a CDP or OCSP response fails, then Solution Components must use the current cached CRL or OCSP response.	T=O		All
KM-CR-30	If a using a CDP and the CDP is offline or contains an invalid CRL, then Inner and Outer Solution Component CRLs must be manually updated prior to the expiration of the current cached CRLs.	T=O		All
KM-CR-31	If using CDPs/OCSP Responders, CDPs and OCSP Responders must not provide any other services other than the distribution of CRLs.	T=O		All

6.6 WIRELESS PASSWORD REQUIREMENTS

The following requirements apply to the MA CP using a Retransmission Device and/or Dedicated Outer VPN with wireless connectivity.

Table 99. Wireless Password Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
MA-KM-1	Wireless Passwords used must be 256 bits.	T=O	
MA-KM-2	Wireless Passwords must be generated by NSA-approved solutions.	T=O	
MA-KM-3	Wireless Passwords must be distributed to and installed on CSfC devices in a manner that minimizes the exposure of the Wireless Password to the greatest extent possible.	T=O	
MA-KM-4	Wireless Passwords must be periodically updated based on the threat environment. The higher the threat environment, the more often the Wireless Passwords are to be updated. At a minimum, Wireless Passwords must be updated once per year.	T=O	
MA-KM-5	A Wireless Password must be updated on all CSfC devices that use the Wireless Password as soon as practically possible if the Wireless Password is considered or suspected to be compromised.	T=O	
MA-KM-6	If a Wireless Password is considered or suspected to be compromised, the solution components must not accept traffic from devices using that Wireless Password until a new Wireless Password is provisioned.	T=O	

6.7 CAMPUS WLAN CP KEY MANAGEMENT REQUIREMENTS

The following requirements apply to the WLAN CP.

Table 1010. Campus WLAN CP Key Management Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
WLAN-KM-1	The Outer CA must issue certificates to the WLAN Authentication Server that contains the TLS Web Server Authentication OID (1.3.6.1.5.5.7.3.1) in the ExtendedKeyUsage certificate extension.	T=O		All
WLAN-KM-2	The Outer CA must issue certificates to the WLAN Client that contains the TLS Web Client Authentication (OID 1.3.6.1.5.5.7.3.2) ExtendedKeyUsage certificate extension.	T=O		All

6.8 MACSEC KEY MANAGEMENT REQUIREMENT

The following requirement applies to the MSC CP when the MACsec protocol is used with pre-shared Connectivity Association Keys (CAKs).

Table 1111. MACsec Key Management Requirement

Req #	Requirement Description	Threshold / Objective	Alternative
MSC-KM-1	If the MACsec protocol is used with pre-shared Connectivity Association Keys (CAKs), all threshold requirements in the *CSfC Symmetric Key Management Requirements Annex* must be met.	T=O	

6.9 ENTERPRISE GRAY KEY MANAGEMENT REQUIREMENTS

Table 1212. Enterprise Gray Annex Key Management Requirements

Req #	Requirement Description	Threshold / Objective	Alternative
EG-KM-1	For CSfC solutions that deploy central management in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) must use a certificate issued by a different CA than the Inner CA for authentication.	T=O	
EG-KM-2	For CSfC solutions that deploy central management in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) and the Outer Encryption Component must use certificates issued by the same Outer CA for authentication.	T	EG-KM-3 EG-KM-4

Req #	Requirement Description	Threshold / Objective	Alternative
EG-KM-3	For CSfC solutions that deploy central management in accordance with *the CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) must use a certificate issued by a different CA than the Outer Encryption Component for authentication.	O	EG-KM-2 EG-KM-4
EG-KM-4	For CSfC solutions that deploy central management in accordance with the *CSfC Enterprise Gray Implementation Requirements Annex*, the Gray Firewall (used as the Inner VPN Gateway for the management plane) OR the Outer Encryption Component must use a 256-bit PSK for authentication. See the *CSfC Symmetric Key Management Requirements Annex* for additional requirements related to the use of PSKs.	O	EG-KM-2 EG-KM-3

7 ROLE-BASED PERSONNEL REQUIREMENTS

Registration Authority (RA) – The RA is an entity authorized by the CA to collect, verify, and submit information that is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. The RA role can be combined with the CAA role. RA duties include, but are not limited to the following:

1) Verify the accuracy of information included in certificate requests.
2) Approve and execute the issuance of certificates.
3) Request, approve, and execute the revocation of certificates.

Certification Authority Administrator (CAA) – The CAA must maintain, monitor, and control all security functions for the CA products. The CAA role can be combined with the RA role. CAA duties include, but are not limited to:

1) Install, configure, and maintain the CA.
2) Configure certificate profiles or templates and audit parameters.
3) Maintain CA operating system and application accounts.
4) Routine operation of the CA equipment such as system backup and recovery.
5) Authorize RAs and approve certificates issued to RAs.
6) Control and manage CA cryptographic modules (e.g., HSMs).
7) Maintain and update the CRL.

8) Provision and maintain certificates in accordance with this Annex for implementations that use them.

Auditor – The Auditor is responsible to review the events recorded in the audit logs to ensure that no action or event represents a compromise to the security of the CAs and CSfC solution. Auditor duties include, but are not limited to, the following:

1) Review, manage, control, and maintain security audit log data.

2) Document and report security-related incidents to the appropriate authorities.

Security Administrator – This role is defined in each of the CPs that this Annex applies to.

Table 1313. Role-Based Personnel Requirements

Req #	Requirement Description	Threshold / Objective	Alternative	CA Type
KM-RB-1	CAAs, RAs, and Auditors must be cleared to the highest level of data protected by the CSfC solution. When an Enterprise CA is used in the solution, the CAA, RA, and Auditor already in place may also support this CSfC solution and use their current practices, provided they meet this requirement.	T=O		All
KM-RB-2	The Auditor role and Security Administrator role must not be combined with any other trusted roles defined in this Annex.	T=O		All
KM-RB-3	All personnel holding trusted roles must meet local Information Assurance (IA) training requirements.	T=O		All
KM-RB-4	The CAA(s)/RA(s) for the Inner Tunnel CA must be different individuals from the CAA(s)/RA(s) for the Outer Tunnel CA.	T=O		All
KM-RB-5	Upon notification of a lost or stolen device, the RA must revoke that device's certificates.	T=O		All
KM-RB-6	Auditing of the Outer and Inner Tunnel CA operations must be performed by individuals who were not involved in the development of the Certificate Policy and Certification Practice Statement (CPS), or integration of the CSfC solution.	T=O		All
KM-RB-7	Mandatory Access Control policy must specify roles for CAAs, RAs, and Auditors using role-based access controls.	O	Objective Only	All
KM-RB-8	Separate RA workstations must be used for the Inner and Outer CAs.	O	Objective Only	All

8 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a CSfC solution. This T&E will be a critical part of the approval process for the AO, providing a robust body of evidence that shows compliance with this Annex.

The security features and operational capabilities associated with the use of the solution must be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the CSfC solution. The entire solution is addressed by this test plan including the following:

1) Set up the baseline network and configure all components.

2) Document the baseline network configuration. Include product model and serial numbers, software version numbers, and software configuration settings at a minimum.

3) Develop a test plan for the specific implementation using the test requirements from Table 13. Any additional requirements imposed by the local AO should also be tested, and the test plan must include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.

4) Perform testing using the test plan derived in Step 3. Network testing will consist of both Black box testing and Gray box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution must be documented.

5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a Final Test Report to be delivered to the AO for approval of the solution.

The following testing requirement has been developed to ensure that the CSfC solution functions properly and meets the requirements defined in this Annex. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 1414. Test Requirement

Req #	Requirement Description	Threshold / Objective	Alternative
KM-TR-1	The organization implementing the Annex must perform all tests listed in the KM Annex Test Annex. T=O	T=O	

APPENDIX A. PASSWORD/PASSPHRASE STRENGTH PARAMETERS

This appendix provides password and passphrase parameters for use in CSfC solutions to address attacks directly based on the strength of the password or passphrase. The information below, describes the factors that provide strength to passwords and passphrases, and sets a minimum standard for use.

Strength

Entropy is used as a measure of strength for passwords and passphrases. According to NIST SP 800-63-2, *Electronic Authentication Guideline*, entropy is a measure of the amount of uncertainty that an attacker faces to determine the value of the secret. Entropy is usually stated in bits; for example, an unpredictable password with 10 bits of entropy would have 2^{10} or 1,024 possible combinations. The greater the number of possible combinations, the greater the amount of time on average it will take an attacker to find the correct password or passphrase.

Random vs. User Generated

Passwords and passphrases are required to be randomly generated. A randomly generated value has the benefit that it will provide an objective amount of entropy, but can be difficult for a user to remember. A user generated value may be easier to remember, but may be predictable, therefore, lowering the entropy calculation reducing the strength of the password or passphrase. If random generation is not a workable solution for the mission use case, then a deviation is required. There are many suggested methods for the user generation of passwords; more information on these can be found in NIST SP 800-118, *Guide to Enterprise Password Management*. These methods attempt to reduce the predictability while maintaining length and memorability, but because they are user chosen, they are all still at risk of being predicable. If the password or passphrase is predicable, an attacker could try a much shorter list of common or personal values, reducing the average time to find the correct password or passphrase. The most effective way to ensure the password or passphrase has an appropriate amount of entropy is by applying random generation. The remainder of this appendix addresses random generation.

Randomly Generated Passwords

The strength of a password is determined by the character set and the length. The character set describes the group of unique characters that may be chosen to create the password, such as numbers, lower case letters, upper case letters, special characters, etc. The length simply describes the number of characters chosen.

Randomly Generated Passphrases

The strength of a passphrase is determined by the number of words in the passphrase and the number of words in the word list, the pool of unique words that can be chosen for the passphrase. The word list can be adjusted by the properties of the words it includes, such as minimum word length, maximum word length, and complexity (includes factors such as the difficulty of the word, capitalization, character substitutions, etc.) per word. Each property has a tradeoff between strength and usability. A minimum word length of four is recommended to maintain the effectiveness of the passphrase. This is based on entropy per word from a word list ranging from 10,000 to 450,000, and entropy per character from a

character set of 26. This ensures the entropy per set of characters of a given word is greater than the entropy provided from selecting a word from the word list.

Multi-Factor Authentication

If a password/passphrase is being used as part of a multi-factor authentication solution and another factor is being used as a primary factor for that component, then the password or passphrase does not need to comply with these rules. It is still recommended to comply with these rules. If the other factor is not a primary factor and used as secondary, these rules still apply.

Assumptions

When using a password/passphrase with the DAR CP, the product the password/passphrase is entered into is assumed to meet one of the DAR protection profiles. All password and passphrase conditioning assumes salting is performed, making pre-computed attacks infeasible. A salt is a random value that is used in a cryptographic process to ensure that the results of the computations for one instance cannot be reused by an attacker. The product is assumed to be kept up to date and the protection mechanisms used in calculations cannot be bypassed.

Minimum Strength Calculations

CSfC provides a tool for random generation, which is available on GitHub at https://github.com/nsacyber/RandPassGenerator. This tool or an alternative NSA-approved tool must be used to generate random passwords and passphrases. When using this tool to generate passwords and passphrases, it should be run on a network capable of protecting the classification of the data that is being protected. The tool should be sent to the appropriate classified network through an AO approved controlled interface for further use. During registration instructions on how to download, verify, and use the tool will be provided. Alternatively, contact the CSfC PMO at csfc_register@nsa.gov for further instructions. The provided tool is set to a default strength of 160 bits, this may be set lower, but must not be set below 112 bits. If using custom word lists or character sets and not using the provided tool, Table 14 and Table 15 show the required minimum length of a password and passphrase given a set of characters or words. The provided tool is capable of utilizing custom word lists. The user must define the size of the character set or word list they will use. To use the tables, find the value that is less than or equal to your character set (or word list) size in the Character Set Size (or Word List Size) column and the corresponding value in the Minimum Password Length (or Minimum Passphrase Length) column for that row reflects the minimum password (or passphrase) length that must be used.

Table 15: Randomly Generated Minimum Password Length

Randomly Generated Passwords	
Character Set Size	**Minimum Password Length**
75	16
58	17
47	18
38	19
32	20
27	21

Randomly Generated Passwords	
Character Set Size	**Minimum Password Length**
23	22
21	23
18	24
16	25
15	26
13	27
12	28
11	29
10	30

460

461 **Table 16: Randomly Generated Minimum Passphrase Length**

Randomly Generated Passphrases	
Word List Size	**Minimum Passphrase Length**
1000000	5
100000	6
20000	7
6000	8
2200	9
1000	10

462

463

APPENDIX B. ACRONYMS

Acronym	Meaning
AO	Authorizing Official
CA	Certification Authority
CAK	Connectivity Association Key
CDP	CRL Distribution Point
CDS	Cross Domain Solution
CEK	CAK Encryption Key
CKN	Connectivity Association Key Name
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CP	Capability Package
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
DAR	Data-At-Rest
DIT	Data-In-Transit
DM	Device Management
DN	Domain Name
ECDH	Elliptic Curve Diffie-Hellman
EAP	Extensible Authentication Protocol
EST	Enrollment Over Secure Transport
EUD	End User Device
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
KGS	Key Generation Solution
KM	Key Management
KMI	Key Management Infrastructure
MA	Mobile Access
MACsec	Media Access Control Security
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security Systems
O	Objective
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PSK	Pre-shared Key
RA	Registration Authority
RFC	Request for Comment
SSH	Secure Shell

Acronym	Meaning
SSHv2	Secure Shell Version 2
T	Threshold
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access III

465

APPENDIX C. REFERENCES

Document	Title	Date
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CNSSD 506	*CNSS Directive (CNSSD) 506, National Directive to Implement Public Key Infrastructure on Secret Networks*	January 2019
CNSSI 1300	*CNSSI 1300, National Security Systems Public Key Infrastructure X.509 Certificate Policy*	December 2014
CNSSI 4009	*CNSSI 4009, Committee for National Security Systems (CNSS) Glossary*	April 2015
CNSSP 7	*CNSS Policy (CNSSP) Number 7, National Policy on the Use of Commercial Solutions to Protect National Security Systems*	December 2015
CNSSP 11	*CNSS Policy (CNSSP) Number 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*	June 2013
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Policy on the Use of Public Standards for Secure Information Sharing*	October 2016
CNSSP 25	*CNSS Policy (CNSSP) Number 25, National Policy for Public Key Infrastructure in National Security Systems (NSS)*	December 2017
CSfC Campus WLAN CP	*Commercial Solutions for Classified (CSfC): Campus Wireless Local Area Network (WLAN) Capability Package (CP), v3.1*	January 2025
CSfC EG Annex	*Commercial Solutions for Classified (CSfC): Enterprise Gray Implementation Requirements Annex, v1.1*	May 2022
CSfC MA CP	*Commercial Solutions for Classified (CSfC): Mobile Access Capability Package (CP), v2.7*	January 2025
CSfC MSC CP	*Commercial Solutions for Classified (CSfC): Multi-Site Connectivity (MSC) Capability Package (CP), v1.2*	March 2023
CSFC SKM Annex	*Commercial Solutions for Classified (CSfC): Symmetric Key Management Requirements Annex, v2.1*	May 2022
FIPS 140	*Federal Information Processing Standard 140, Security Requirements For Cryptographic Modules National Institute for Standards and Technology FIPS Publication*	March 2019
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	August 2015
FIPS 186	*Federal Information Processing Standard 186-4, Digital Signature Standard (DSS)*	July 2013
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
IR 7924	*NIST Interagency Report (IR) 7924, Reference Certificate Policy, Second Draft.* H. Booth and A. Regenscheid.	May 2014

Document	Title	Date
PP CA	*Protection Profile for Certification Authorities*. http://www.niap-ccevs.org/pp	December 2017
RFC 3647	*IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Internet Engineering Task Force.* S. Chokhani, et. al.	November 2003
RFC 4308	*IETF RFC 4308 Cryptographic Suites for IPsec.* P. Hoffman.	December 2005
RFC 4754	*IETF RFC 4754 IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*. D. Fu and J. Solinas.	January 2007
RFC 5216	*IETF RFC 5216 The EAP-TLS Authentication Protocol.* D. Simon, B.Aboba, and R. Hurst.	March 2008
RFC 5246	*IETF RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2*. T. Dierks and E. Rescorla.	August 2008
RFC 5280	*IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. D. Cooper, et. al.	May 2008
RFC 6818	*IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. P. Yee	January 2013
RFC 6960	*IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP,* S. Santesson, et. al.	June 2013
RFC 7030	*IETF RFC 7030 Enrollment over Secure Transport*. M. Pritikin, P. Yee, and D. Harkins.	October 2013
RFC 7296	*IETF RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2). C. Kaufman, et. al.*	October 2014
RFC 8247	*IETF RFC 8247 Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2).* Y. Nir, et. al.	September 2017
RFC 8295	*IETF RFC 8295 EST (Enrollment over Secure Transport) Extensions* S. Turner.	January 2018
RFC 8422	*IETF RFC 8422 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier.* Y. Nir, et. al.	August 2018
RFC 8446	*IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3.* E. Rescorla.	August 2018
RFC 8603	*IETF RFC 8603 Commercial National Security Algorithm (CNSA) Suite Certificate and Certificate Revocation List (CRL) Profile.* M. Jenkins, and L. Zieglar.	May 2019
RFC 9151	*IETF RFC 9151 Commercial National Security Algorithm (CNSA) Profile for TLS and DTLS 1.2 and 1.3.* D. Cooley.	April 2022
RFC 9152	*IETF RFC 9152 The SODP (Secure Object Delivery Protocol) Server Interfaces: NSA's Profile for Delivery of Certificates, CRLs, and Symmetric Keys to Clients.* S. Turner, M. Jenkins.	April 2022

Document	Title	Date
SP 800-53	*NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations*. Joint Task Force Transformation Initiative.	April 2013
SP 800-56A	*NIST Special Publication 800-56A Rev. 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. E. Barker, et. al.	April 2018
SP 800-56B	*NIST Special Publication 800-56B Rev. 2, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. E. Barker, et. al.	March 2019
SP 800-56C	*NIST Special Publication 800-56C Rev. 2, Recommendation for Key Derivation through Extraction-then-Expansion*. E. Barker, et. al.	August 2020
SP 800-57-1	*NIST Special Publication 800-57 Part 1 Rev. 5, Recommendation for Key Management - General.* E. Barker.	May 2020
SP 800-57-2	*NIST Special Publication 800-57 Part 2 Rev. 1, Recommendation for Key Management – Best Practices for Key Management Organizations.* E. Barker, et. al.	May 2019
SP 800-57-3	*NIST Special Publication 800-57 Part 3 Rev. 1, Recommendation for Key Management – Application-Specific Key Management Guidance.* E. Barker, et. al.	Jan 2015
SP 800-77	*NIST Special Publication 800-77 Rev. 1, Guide to IPsec VPNs.* E. Barker, et. al.	June 2020
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths*. E. Barker.	March 2019

467

468